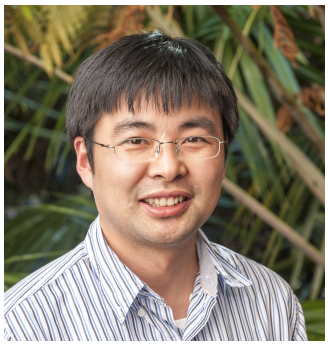
YANG Guomin

School of Computing and Information Systems
Singapore Management University (SMU)
80 Stamford Road
Singapore 178902

Email: gmyang@smu.edu.sg
Office Phone: (+65) 68264928



Education

PhD, City University of Hong Kong, China, 2009

MPhil, City University of Hong Kong, China, 2006

Bachelor of Science, City University of Hong Kong, China, 2004

Academic Appointments

Associate Professor of Computer Science, School of Computing and Information Systems, SMU, Aug 2022 - Present

Academic Administrative Positions

Coordinator, BSc (CS) Cybersecurity Track, School of Computing and Information Systems, SMU, Jul 2023 - Present

RESEARCH

Publications

Journal Articles [Refereed]

STDA: Secure Time Series Data Analytics with practical efficiency in wide-area network, by LI, Xiaoguo; HUANG Zixi; ZHAO, Bowen; YANG, Guomin; XIANG, Tao; DENG, Robert H.. (2023). *IEEE Transactions on Information Forensics and Security, 19* 1440-1454. (Published)

Policy-Based Remote User Authentication From Multi-Biometrics, by TIAN, Yangguang; LI, Yingjiu; DENG, Robert H.; YANG, Guomin; LI, Nan. (2023). *Computer Journal,* https://doi.org/10.1093/comjnl/bxad102 (Advance Online)

Fair cloud auditing based on blockchain for resource-constrained IoT devices, by ZHOU, Lei.; FU, Anmin.; YANG, Guomin.; GAO, Yansong.; YU, Shui.; DENG, Robert H.. (2023). *IEEE Transactions on Dependable and Secure Computing, 20* (5), 4325-4342. https://doi.org/10.1109/TDSC.2022.3207384 (Published)

Privacy-Preserving Multi-User Outsourced Computation for Boolean Circuits, by LIU, Xueqiao.; YANG, Guomin.; SUSILO, Willy.; HE, Kai.; DENG, Robert H.; WENG, Jian.. (2023). *IEEE Transactions on Information Forensics and Security, 18* 4929-4943. (Published)

Balancing privacy and flexibility of cloud-based personal health records sharing system, by ZHANG, Yudi;

GUO, Fuchun; SUSILO, Willy; YANG, Guomin. (2023). *IEEE Transactions on Cloud Computing, 11* (3), 2420-2430. https://doi.org/10.1109/TCC.2022.3208168 (Published)

Generic conversions from CPA to CCA without ciphertext expansion for threshold ABE with constant-size ciphertexts, by LAI, J; GUO, F; SUSILO, W; JIANG, P; YANG, G;HUANG, X.. (2022). *Information Sciences, 613* 966-981. https://doi.org/10.1016/j.ins.2022.08.069 (Published)

Secure Deterministic Wallet and Stealth Address: Key-Insulated and Privacy-Preserving Signature Scheme With Publicly Derived Public Key, by LIU, Zhen; YANG, Guomin; WONG, Duncan S.; NGUYEN, Khoa; WANG, Huaxiong; KE, Xiaorong; LIU, Yining. (2022). *IEEE Transactions on Dependable and Secure Computing, 19* (5), 2934-2951. http://doi.org/10.1109/TDSC.2021.3078463 (Published)

Sanitizable Access Control System for Secure Cloud Storage Against Malicious Data Publishers, by SUSILO, Willy; JIANG, Peng; LAI, Jianchang; GUO, Fuchun; YANG, Guomin; DENG, Robert H.. (2022). *IEEE Transactions on Dependable and Secure Computing, 19* (3), 2138-2148. https://doi.org/10.1109/TDSC.2021.3058132 (Published)

Message-Locked Searchable Encryption: A New Versatile Tool for Secure Cloud Storage, by LIU, Xueqiao; YANG, Guomin; SUSILO, Willy; TONIEN, Joseph; CHEN, Rongmao; LV, Xixiang. (2022). *IEEE Transactions on Services Computing, 15* (3), 1664-1677. http://doi.org/10.1109/TSC.2020.3006532 (Published)

Efficient Certificateless Multi-Copy Integrity Auditing Scheme Supporting Data Dynamics, by ZHOU, Lei; FU, Anmin; YANG, Guomin; WANG, Huaqun; ZHANG, Yuqing. (2022). *IEEE Transactions on Dependable and Secure Computing, 19* (2), 1118-1132. http://doi.org/10.1109/TDSC.2020.3013927 (Published)

A Blockchain-Based Self-Tallying Voting Protocol in Decentralized IoT, by LI, Yannan; SUSILO, Willy; YANG, Guomin; YU, Yong; LIU, Dongxi; DU, Xiaojiang; GUIZANI, Mohsen. (2022). *IEEE Transactions on Dependable and Secure Computing, 19* (1), 119-130. http://doi.org/10.1109/TDSC.2020.2979856 (Published)

Functional signatures: new definition and constructions, by GUO, Qingwen; HUANG, Qiong; MA, Sha; XIAO, Meiyan; YANG, Guomin; SUSILO, Willy. (2021). *SCIENCE CHINA Information Sciences, 64* (12), 1-13. http://doi.org/10.1007/s11432-019-2855-3 (Published)

Efficient Server-Aided Secure Two-Party Computation in Heterogeneous Mobile Cloud Computing, by WU, Yulin; WANG, Xuan; SUSILO, Willy; YANG, Guomin; JIANG, Zoe L.; CHEN, Qian; XU, Peng. (2021). *IEEE Transactions on Dependable and Secure Computing, 18* (6), 2820-2834. http://doi.org/10.1109/TDSC.2020.2966632 (Published)

Privacy-preserving voluntary-tallying leader election for internet of things, by WU, Tong; YANG, Guomin; ZHU, Liehuang; WU, Yulin. (2021). *Information Sciences, 574* 461-472. (Published)

Unlinkable and Revocable Secret Handshake, by TIAN, Yangguang; LI, Yingliu; MU, Yi; YANG, Guomin. (2021). *Computer Journal, 64* (8), 1303-1314. https://doi.org/10.1093/comjnl/bxaa181 (Published)

Privacy-Preserving Proof of Storage for the Pay-As-You-Go Business Model, by WU, Tong; YANG, Guomin; MU, Yi; GUO, Fuchun; DENG, Robert H.. (2021). *IEEE Transactions on Dependable and Secure Computing, 18* (2), 563-575. https://doi.org/10.1109/TDSC.2019.2931193 (Published)

Lattice-based remote user authentication from reusable fuzzy signature, by TIAN, Yangguang; LI, Yingjiu; DENG, Robert H.; SENGUPTA, Binanda; YANG, Guomin
. (2021). *Journal of Computer Security, 29* (3), 273-298. (Published)

Traceable Monero: Anonymous Cryptocurrency with Enhanced Accountability, by LI, Yannan; YANG, Guomin; SUSILO, Wily; YU, Yong; AU, Man Ho; LIU, Dongxi. (2021). *IEEE Transactions on Dependable and Secure Computing, 18* (2), 679-691. https://doi.org/10.1109/TDSC.2019.2910058 (Published)

Privacy-Preserving Multi-Keyword Searchable Encryption for Distributed Systems, by LIU, Xueqiao; YANG, Guomin; SUSILO, Willy; TONIEN, Joseph; SHEN, Jian. (2021). *IEEE Transactions on Parallel and Distributed Systems, 32* (3), 561-574. http://doi.org/10.1109/TPDS.2020.3027003 (Published)

Divide and capture: An improved cryptanalysis of the encryption standard algorithm RSA, by SUSILO, Willy; TONIEN, Joseph; YANG, Guomin. (2021). *Computer Standards & Interfaces, 74* 1-6. http://doi.org/10.1016/j.csi.2020.103470 (Published)

An Efficient Privacy Preserving Message Authentication Scheme for Internet-of-Things, by WEI, Jiannan; PHUONG, Tran Viet Xuan; YANG, Guomin. (2021). *IEEE Transactions on Industrial Informatics, 17* (1),

617-626. http://doi.org/10.1109/TII.2020.2972623 (Published)

Multi-User Verifiable Searchable Symmetric Encryption for Cloud Storage, by LIU, Xueqiao; YANG, Guomin; DENG, Robert H. . (2020). *IEEE Transactions on Dependable and Secure Computing, 17* (6), 1322-1332. http://doi.org/10.1109/TDSC.2018.2876831 (Published)

Hierarchical Identity-Based Signature in Polynomial Rings, by YANG, Zhichao; DUONG, Dung H.; SUSILO, Willy; YANG, Guomin; LI, Chao; CHEN, Rongmao. (2020). *Computer Journal, 63* (10), 1490-1499. http://doi.org/10.1093/comjnl/bxaa033 (Published)

Efficient Fine-Grained Data Sharing Mechanism for Electronic Medical Record Systems with Mobile Devices, by MA, Hui; ZHANG, Rui; YANG, Guomin; ZONG, Zishuai; HE, Kai; XIAO, Yuting. (2020). *IEEE Transactions on Dependable and Secure Computing, 17* (5), 1026-1038. http://doi.org/10.1109/TDSC.2018.2844814 (Published)

A generalised bound for the Wiener attack on RSA, by SUSILO, Willy; TONIEN, Joseph; YANG, Guomin. (2020). *Journal of Information Security and Applications, 53* 1-4. http://doi.org/10.1016/j.jisa.2020.102531 (Published)

Privacy-enhanced remote data integrity checking with updatable timestamp, by WU, Tong; YANG, Guomin; MU, Yi; CHEN, Rongmao; XU, Shengmin. (2020). *Information Sciences, 527* 210-226. https://doi.org/10.1016/j.ins.2020.03.057 (Published)

A New Construction for Linkable Secret Handshake, by TIAN, Yangguang; LI, Yingjiu; DENG, Robert H.; LI, Nan; YANG, Guomin; YANG, Zheng. (2020). *Computer Journal, 63* (4), 536-548. https://doi.org/10.1093/comjnl/bxz095 (Published)

Attribute-Based Cloud Data Integrity Auditing for Secure Outsourced Storage, by YU, Yong; LI, Yannan; YANG, Bo; SUSILO, Willy; YANG, Guomin; BAI, Jian. (2020). *IEEE Transactions on Emerging Topics in Computing, 8* (2), 377-390. http://doi.org/10.1109/TETC.2017.2759329 (Published)

Energy-Efficient Distance-Bounding with Residual Charge Computation, by ZHUANG, Yunhui; YANG, Anjia; HANCKE, Gerhard; WONG, Duncan S.; YANG, Guomin. (2020). *IEEE Transactions on Emerging Topics in Computing, 8* (2), 365-376. http://doi.org/10.1109/TETC.2017.2761702 (Published)

On the Security of LWE Cryptosystem against Subversion Attacks, by YANG, Zhichao; CHEN, Rongmao; LI, Chao; QU, Longjiang; YANG, Guomin. (2020). *Computer Journal, 63* (4), 495-507. http://doi.org/10.1093/comjnl/bxz084 (Published)

Strongly leakage resilient authenticated key exchange, revisited, by YANG, Guomin; CHEN, Rongmao; MU, Yi; SUSILO, Willy; GUO Fuchun; LI, Jie. (2019). *Designs, Codes and Cryptography, 87* (12), 2885-2911. http://doi.org/10.1007/s10623-019-00656-3 (Published)

ESDRA: An Efficient and Secure Distributed Remote Attestation Scheme for IoT Swarms, by KUANG, Boyu; FU, Anmin; YU, Shui; YANG, Guomin; SU, Mang; ZHANG, Yuqing. (2019). *IEEE Internet of Things Journal, 6* (5), 8372-8383. http://doi.org/10.1109/JIOT.2019.2917223 (Published)

A secure IoT cloud storage system with fine-grained access control and decryption key exposure resistance, by XU, Shengmin; YANG, Guomin; MU, Yi; LIU, Ximeng. (2019). *Future Generation Computer Systems: The International Journal of eScience, 97* 284-294. https://doi.org/10.1016/j.future.2019.02.051 (Published)

Designated-server identity-based authenticated encryption with keyword search for encrypted emails, by LI, Hongbo; HUANG, Qiong; SHEN, Jian; YANG, Guomin; SUSILO, Willy. (2019). *Information Sciences, 481* 330-343. http://doi.org/10.1016/j.ins.2019.01.004 (Published)

Revocable attribute-based encryption with decryption key exposure resistance and ciphertext delegation, by XU, Shengmin; YANG, Guomin; MU, Yi. (2019). *Information Sciences, 479* 116-134. https://doi.org/10.1016/j.ins.2018.11.031 (Published)

DABKE: Secure deniable attribute-based key exchange framework, by TIAN, Yangguang; LI, Yingjiu; YANG, Guomin; SUSILO, Willy; MU, Yi; CUI, Hui; ZHANG, Yinghui. (2019). *Journal of Computer Security, 27* (2), 259-275. https://doi.org/10.3233/JCS-181201 (Published)

Authorized Function Homomorphic Signature, by GUO, Qingwen; HUANG, Qiong; YANG, Guomin. (2018). *Computer Journal, 61* (12), 1897-1908. http://doi.org/10.1093/comjnl/bxy114 (Published)

Exploring relationship between indistinguishability-based and unpredictability-based RFID privacy models, by YANG, Anjia; ZHUANG, Yunhui; WENG, Jian; HANCKE, Gerhard; WONG, Duncan S.; YANG, Guomin. (2018). *Future Generation Computer Systems: The International Journal of eScience, 82* 315-326. http://doi.org/10.1016/j.future.2017.12.044 (Published)

Criteria-Based Encryption, by PHUONG, Tran Viet Xuan; YANG, Guomin; SUSILO, Willy. (2018). *Computer Journal, 61* (4), 512-525. http://doi.org/10.1093/comjnl/bxx088 (Published)

A New Revocable and Re-Delegable Proxy Signature and Its Application, by XU, Shengmin; YANG, Guomin; MU, Yi. (2018). *Journal of Computer Science and Technology, 33* (2), 380-399. https://doi.org/10.1007/s11390-018-1825-4 (Published)

Constant-size ciphertexts in threshold attribute-based encryption without dummy attributes, by SUSILO, Willy; YANG, Guomin; GUO, Fuchun; HUANG, Qiong. (2018). *Information Sciences, 429* 349-360. http://doi.org/10.1016/j.ins.2017.11.037 (Published)

Strong Identity-Based Proxy Signature Schemes, Revisited, by LIU, Weiwei; MU, Yi; YANG, Guomin; TIAN, Yangguang. (2018). *Wireless Communications and Mobile Computing, 2018* 1-11. https://doi.org/10.1155/2018/6925019 (Published)

EACSIP: Extendable Access Control System With Integrity Protection for Enhancing Collaboration in the Cloud, by SUSILO, Willy; JIANG, Peng; GUO, Fuchun; YANG, Guomin; YU, Yong; MU, Yi. (2017). *IEEE Transactions on Information Forensics and Security, 12* (12), 3110-3122. http://doi.org/10.1109/TIFS.2017.2737960 (Published)

Strong authenticated key exchange with auxiliary inputs, by CHEN, Rongmao; MU, Yi; YANG, Guomin; SUSILO, Willy; GUO, Fuchun. (2017). *Designs, Codes and Cryptography, 85* (1), 145-173. http://doi.org/10.1007/s10623-016-0295-3 (Published)

Sequence aware functional encryption and its application in searchable encryption, by PHUONG, Tran Viet Xuan; YANG, Guomin; SUSILO, Willy; GUO, Fuchun; HUANG, Qiong. (2017). *Journal of Information Security and Applications, 35* 106-118. https://doi.org/10.1016/j.jisa.2017.06.002 (Published)

A new public remote integrity checking scheme with user and data privacy, by FENG, Yiteng; MU, Yi; YANG, Guomin; LIU, Joseph. (2017). *International Journal of Applied Cryptography, 3* (3), 196-209. http://doi.org/10.1504/IJACT.2017.086232 (Published)

RFID Ownership Transfer with Positive Secrecy Capacity Channels, by MUNILLA, Jorge; BURMESTER, Mike; PEINADO, Alberto; YANG, Guomin; SUSILO, Willy. (2017). *Sensors, 17* (1), http://doi.org/10.3390/s17010053 (Published)

Server-Aided Public Key Encryption With Keyword Search, by CHEN, Rongman; MU, Yi; YANG, Guomin; GUO, Fuchun; HUANG, Xinyi; WANG, Xiaofen; WANG, Yongjun. (2016). *IEEE Transactions on Information Forensics and Security, 11* (12), 2833-2842. http://doi.org/10.1109/TIFS.2016.2599293 (Published)

Anonymous Proxy Signature with Hierarchical Traceability, by WEI, Jiannan; YANG, Guomin; MU, Yi; LIANG, Kaitai. (2016). *Computer Journal, 59* (4), 559-569. http://doi.org/10.1093/comjnl/bxv080 (Published)

Dual-Server Public-Key Encryption With Keyword Search for Secure Cloud Storage, by CHEN, Rongmao; MU, Yi; YANG, Guomin; GUO, Fuchun; WANG, Xiaofen. (2016). *IEEE Transactions on Information Forensics and Security, 11* (4), 789-798. http://doi.org/10.1109/TIFS.2015.2510822 (Published)

Hidden Ciphertext Policy Attribute-Based Encryption Under Standard Assumptions, by PHUONG, Tran Viet Xuan; YANG, Guomin; SUSILO, Willy. (2016). *IEEE Transactions on Information Forensics and Security, 11* (1), 35-45. http://doi.org/10.1109/TIFS.2015.2475723 (Published)

BL-MLE: Block-Level Message-Locked Encryption for Secure Large File Deduplication, by CHEN, Rongmao; MU, Yi; YANG, Guomin; GUO, Fuchun. (2015). *IEEE Transactions on Information Forensics and Security, 10* (12), 2643-2652. http://doi.org/10.1109/TIFS.2015.2470221 (Published)

On Indistinguishability in Remote Data Integrity Checking, by FAN, Xinyu; YANG, Guomin; MU, Yi; YU, Yong. (2015). *Computer Journal, 58* (4), 823-830. http://doi.org/10.1093/comjnl/bxt137 (Published)

Analysis and Improvement on a Biometric-Based Remote User Authentication Scheme Using Smart Cards, by WEN, Fengtong; SUSILO, Willy; YANG, Guomin. (2015). *Wireless Personal Communications, 80* (4), 1747-1760. https://doi.org/10.1007/s11277-014-2111-6 (Published)

Ambiguous optimistic fair exchange: Definition and constructions, by HUANG, Qiong; YANG, Guomin; WONG, Duncan S.; SUSILO, Willy. (2015). *Theoretical Computer Science, 562* 177-193. http://doi.org/10.1016/j.tcs.2014.09.043 (Published)

Identity based identification from algebraic coding theory, by YANG, Guomin; TAN, Chik How; MU, Yi; SUSILO, Willy; WONG, Duncan S.. (2014). *Theoretical Computer Science, 520* 51-61. http://doi.org/10.1016/j.tcs.2013.09.008 (Published)

Cross-Domain Password-Based Authenticated Key Exchange Revisited, by CHEN, Liqun; LIM, Hoon Wei; YANG, Guomin. (2014). *ACM Transactions on Information and System Security, 16* (4), http://doi.org/10.1145/2584681 (Published)

A robust smart card-based anonymous user authentication protocol for wireless communications, by WEN, Fengton; SUSILO, Willy; YANG, Guomin. (2014). *Security and Communication Networks, 7* (6), 987-993. http://doi.org/10.1002/sec.816 (Published)

On the security of auditing mechanisms for secure cloud storage, by YU, Yong; NIU, Lei; YANG, Guomin; MU, Yi; SUSILO, Willy. (2014). *Future Generation Computer Systems: The International Journal of eScience, 30* (1), 127-132. https://doi.org/10.1016/j.future.2013.05.005 (Published)

A Secure and Effective Anonymous User Authentication Scheme for Roaming Service in Global Mobility Networks, by WEN, Fengtong; SUSILO, Willy; YANG, Guomin. (2013). *Wireless Personal Communications, 73* (3), 993-1004. http://doi.org/10.1007/s11277-013-1243-4 (Published)

A new efficient optimistic fair exchange protocol without random oracles, by HUANG, Qiong; YANG, Guomin; WONG, Duncan S.; SUSILO, Willy. (2012). *International Journal of Information Security, 11* (1), 53-63. http://doi.org/10.1007/s10207-011-0152-3 (Published)

Certificateless cryptography with KGC trust level 3, by YANG, Guomin; TAN, Chik How. (2011). *Theoretical Computer Science, 412* (39), 5446-5457. http://doi.org/10.1016/j.tcs.2011.06.015 (Published)

Heterogeneous Signcryption with Key Privacy, by HUANG, Qiong; WONG, Duncan S.; YANG, Guomin . (2011). *Computer Journal, 54* (4), 525-536. http://doi.org/10.1093/comjnl/bxq095 (Published)

Certificateless public key encryption: A new generic construction and two pairing-free schemes, by YANG, Guomin; TAN, Chik How . (2011). *Theoretical Computer Science, 412* (8-10), 662-674. http://doi.org/10.1016/j.tcs.2010.10.025 (Published)

Identity-based strong designated verifier signature revisited, by HUANG, Qiong; YANG, Guomin; WONG, Duncan S.; SUSILO, Willy. (2011). *Journal of Systems and Software, 84* (1), 120-129. http://doi.org/10.1016/j.jss.2010.08.057 (Published)

Efficient strong designated verifier signature schemes without random oracle or with non-delegatability, by HUANG, Qiong; YANG, Guomin; WONG, Duncan S.; SUSILO, Willy. (2011). *International Journal of Information Security, 10* (6), 373-385. http://doi.org/10.1007/s10207-011-0146-1 (Published)

An efficient signcryption scheme with key privacy and its extension to ring signcryption, by LI, Chung Ki; YANG, Guomin; WONG, Duncan S.; DENG, Xiaotie; CHOW, Sherman S. M.. (2010). *Journal of Computer Security, 18* (3), 451-473. http://doi.org/10.5555/1835402.1835406 (Published)

Universal Authentication Protocols for Anonymous Wireless Communications, by YANG, Guomin; HUANG, Qiong; WONG, Duncan S.; DENG, Xiaotie. (2010). *IEEE Transactions on Wireless Communications, 9* (1), 168-174. http://doi.org/10.1109/TWC.2010.01.081219 (Published)

A new framework for the design and analysis of identity-based identification schemes, by YANG, Guomin; CHEN, Jing; WONG, Duncan S.; DENG, Xiaotie; WANG, Dongsheng. (2008). *Theoretical Computer Science, 407* (1-3), 370-388. http://doi.org/10.1016/j.tcs.2008.07.001 (Published)

Two-factor mutual authentication based on smart cards and passwords, by YANG, Guomin; WONG, Duncan S.; WANG, Huaxiong; DENG, Xiaotie. (2008). *Journal of Computer and System Sciences, 74* (7), 1160-1172. http://doi.org/10.1016/j.jcss.2008.04.002 (Published)

Anonymous and authenticated key exchange for roaming networks, by YANG, Guomin; WONG, Duncan S.; DENG, Xiaotie. (2007). *IEEE Transactions on Wireless Communications, 6* (9), 3461 -3472. http://doi.org/10.1109/TWC.2007.06020042 (Published)

An efficient identity-based key exchange protocol with KGS forward secrecy for low-power devices, by ZHU, Robert W.; YANG, Guomin; WONG, Duncan S. . (2007). *Theoretical Computer Science, 378* (2), 198-207. http://doi.org/10.1016/j.tcs.2007.02.021 (Published)

Book Chapters

Key establishment — Secrecy, authentication and anonymity, by YANG, Guomin; WONG, Duncan S.; DENG, Xiaotie. (2011). In XIAO, Yang; CHEN, Hui (Ed.), *Handbook of Security and Networks* (pp. 223-244) USA: World Scientific. http://doi.org/10.1142/9789814273046_0008 (Published)

Conference Proceedings

A tightly secure ID-based signature scheme under DL assumption in AGM, by LOH, Jia-Chng; GUO, Fuchun; SUSILO, Willy; YANG, Guomin. (2023.0). *Proceedings of 28th Australasian Conference on Information Security and Privacy (ACISP 2023), Brisbane, Australia, July 5-7,* (pp. 199-219) Switzerland: Springer, Cham. https://doi.org/10.1007/978-3-031-35486-1_10 (Published)

Secure hierarchical deterministic wallet supporting stealth address, by YIN, Xin; LIU, Zhen; YANG, Guomin; CHEN, Guoxing; ZHU, Haojin. (2022.0). *Computer Security ESORICS 2022: 27th European Symposium on Research, Copenhagen, Denmark, September 26-30: Proceedings,* (pp. 89-109) Cham: Springer. https://doi.org/10.1007/978-3-031-17140-6_5 (Published)

Multimodal private signatures, by NGUYEN, Khoa; GUO, Fuchun; SUSILO, Willy; YANG, Guomin . (2022.0). *Advances in Cryptology CRYPTO 2022: 42nd Annual International Conference, Santa Barbara, CA, August 15-18: Proceedings,* (pp. 792-822) Cham: Springer. https://doi.org/10.1007/978-3-031-15979-4_27 (Published)

Concise mercurial subvector commitments: Definitions and constructions, by LI, Yannan; SUSILO, Willy; YANG, Guomin; PHUONG, Tran Viet Xuan; YU, Yong; LIU, Dongxi
. (2021.0). *Information Security and Privacy: 26th Australasian Conference, Virtual Conference, December 1-3: Proceedings,* (pp. 353-371) Cham: Springer. https://doi.org/10.1007/978-3-030-90567-5_18 (Published)

Broadcast authenticated encryption with keyword search, by LIU, Xueqiao; HE, Kai; YANG, Guomin; SUSILO, Willy; TONIEN, Joseph; HUANG, Qiong
. (2021.0). *Information Security and Privacy: 26th Australasian Conference, ACISP 2021, Virtual Conference, December 1-3: Proceedings,* (pp. 193-213) Cham: Springer. https://doi.org/10.1007/978-3-030-90567-5_10 (Published)

SyLPEnIoT: Symmetric lightweight predicate encryption for data privacy applications in IoT environments, by PHUONG, Tran Viet Xuan; SUSILO, Willy; YANG, Guomin; KIM, Jongkil; CHOW, YangWai; LIU, Dongxi . (2021.0). *Computer Security: ESORICS 2021: 26th European Symposium on Research in Computer Security, Darmstadt, Germany, October 4-8: Proceedings,* (pp. 106-126) Cham: Springer. https://doi.org/10.1007/978-3-030-88428-4_6 (Published)

Receiver-anonymity in rerandomizable RCCA-secure cryptosystems resolved, by WANG, Yi; CHEN, Rongmao; YANG, Guomin; HUANG, Xinyi; WANG, Baosheng; YUNG, Moti
. (2021.0). *Advances in Cryptology: CRYPTO 2021: 41st Annual International Cryptology Conference, Virtual, August 16-20: Proceedings,* (pp. 270-300) Cham: Springer. https://doi.org/10.1007/978-3-030-84259-8_10 (Published)

Non-equivocation in blockchain: Double-authentication-preventing signatures gone contractual, by LI, Yannan; SUSILO, Willy; YANG, Guomin; YU, Yong; PHUONG, Tran Viet Xuan; LIU, Dongxi. (2021.0). *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security, Virtual Conference, June 7-11,* (pp. 859-871) Virtual Conference: ACM. http://doi.org/10.1145/3433210.3437516 (Published)

A lattice-based key-insulated and privacy-preserving signature scheme with publicly derived public key, by LIU, Wenling; LIU, Zhen; NGUYEN, Khoa; YANG, Guomin; YU. (2020.0). *Computer Security: ESORICS 2020: 25th European Symposium on Research in Computer Security, Guildford, September 14-18: Proceedings,* (pp. 357-377) Cham: Springer. https://doi.org/10.1007/978-3-030-59013-0_18 (Published)

Generic construction of ElGamal-type attribute-based encryption schemes with revocability and dual-policy, by XU, Shengmin; ZHANG, Yinghui; LI, Yingjiu; LIU, Ximeng; YANG, Guomin. (2019.0).

Proceedings of the 15th EAI International Conference, SecureComm 2019, Orlando, FL, USA, October 23–25, (pp. 184-204) Orlando, FL, USA: Springer Link. https://doi.org/10.1007%2F978-3-030-37231-6_10 (Published)

A lattice-based linkable ring signature supporting stealth addresses, by LIU, Zhen; NGUYEN, Khoa; YANG, Guomin; WANG, Huaxiong; WONG, Duncan S. . (2019.0). *Computer Security: ESORICS 2019: 24th European Symposium on Research in Computer Security, Luxembourg, September 23-27: Proceedings,* (pp. 726-746) Cham: Springer. https://doi.org/10.1007/978-3-030-29959-0_35 (Published)

Puncturable proxy re-encryption supporting to group messaging service, by PHUONG, Tran Viet Xuan; SUSILO, Willy; KIM, Jongkil; YANG, Guomin; LIU, Dongxi
. (2019.0). *Computer Security: 24th European Symposium on Research in Computer Security, ESCORICS 2019, Luxembourg, September 23-27: Proceedings,* (pp. 215-233) Cham: Springer. https://doi.org/10.1007/978-3-030-29959-0_11 (Published)

The Wiener attack on RSA revisited: A quest for the exact bound, by SUSILO, Willy; TONIEN, Joseph; YANG, Guomin. (2019.0). *Information Security and Privacy: 24th Australasian Conference, ACISP 2019, Christchurch, New Zealand, July 3-5: Proceedings,* (pp. 381-398) Cham: Springer. https://doi.org/10.1007/978-3-030-21548-4_21 (Published)

Location based encryption, by PHUONG, Tran Viet Xuan; SUSILO, Willy; YANG, Guomin; YAN, Jun; LIU, Dongxi. (2019.0). *Information Security and Privacy: 24th Australasian Conference, ACISP 2019, Christchurch, New Zealand, July 3-5: Proceedings,* (pp. 21-38) Cham: Springer. https://doi.org/10.1007/978-3-030-21548-4_2 (Published)

Key-insulated and privacy-preserving signature scheme with publicly derived public key, by LIU, Zhen; YANG, Guomin; WONG, Duncan S.; NGUYEN, Khoa; WANG, Huaxiong
. (2019.0). *Proceedings of the 4th IEEE European Symposium on Security and Privacy, Stockholm, Sweden, 2019 June 17-19,* (pp. 1-50) Stockholm, Sweden: IEEE. http://doi.org/10.1109/EuroSP.2019.00025 (Published)

Efficient attribute-based encryption with blackbox traceability, by XU, Shengmin; YANG, Guomin; MU, Yi; LIU, Ximeng. (2018.0). *Proceedings of the 12th International Conference, ProvSec 2018, Jeju, South Korea, October 25–28,* (pp. 182-200) Jeju, South Korea: Springer Link. https://doi.org/10.1007%2F978-3-030-01446-9_11 (Published)

Concessive online/offline attribute based encryption with cryptographic reverse firewalls: Secure and efficient fine-grained access control on corrupted machines, by MA, Hui; ZHANG, Rui; YANG, Guomin; SONG, Zishuai; SUN, Shuzhou; XIAO, Yuting. (2018.0). *Computer Security: 23rd European Symposium on Research in Computer Security, ESORICS 2018, Barcelona, Spain, September 3-7: Proceedings,* (pp. 507-526) Cham: Springer. https://doi.org/10.1007/978-3-319-98989-1_25 (Published)

Optimal security reductions for unique signatures: Bypassing impossibilities with a counterexample, by FUO, Fuchun; CHEN, Rongmao; SUSILO, Willy; LAI, Jianchang; YANG, Guomin; MU, Yi. (2017.0). *Proceedings of the 37th Annual International Cryptology Conference Santa Barbara, USA, 2017 August 20-24,* (pp. 517-547) Santa Barbara: Springer Verlag. http://doi.org/10.1007/978-3-319-63715-0_18 (Published)

Privacy-preserving k-time authenticated secret handshakes, by TIAN, Yangguang; ZHANG, Shiwei; YANG, Guomin; MU, Yi; YU, Yong. (2017.0). *Proceedings of the 22nd Australasian Conference, Auckland, New Zealand, 2017 July 3-5,* (pp. 281-300) Auckland, New Zealand: Springer Verlag. http://doi.org/10.1007/978-3-319-59870-3_16 (Published)

Hierarchical functional encryption for linear transformations, by ZHANG, Shiwei; MU, Yi; YANG, Guomin; WANG, Xiaofen. (2017.0). *Proceedings of the 22nd Australasian Conference, Auckland, New Zealand, 2017 July 3-5,* (pp. 23-43) Auckland, New Zealand: Springer Verlag. http://doi.org/10.1007/978-3-319-60055-0_2 (Published)

Iterated random oracle: A universal approach for finding loss in security reduction, by GUO, Fuchun; SUSILO, Willy; MU, Yi; CHEN, Rongmao; LAI, Jianchang; YANG, Guomin . (2016.0). *Proceedings of the 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, 2016 December 4-8,* (pp. 745-776) Hanoi: Springer Verlag. http://doi.org/10.1007/978-3-662-53890-6_25 (Published)

Cryptographic reverse firewall via malleable smooth projective hash functions, by CHEN, Rongmao; MU, Yi; YANG, Guomin; SUSILO, Willy; GUO, Fuchun; ZHANG, Mingwu. (2016.0). *Proceedings of the 22nd*

International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, 2016 December 4-8, (pp. 844-876) Hanoi: Springer Verlag. http://doi.org/10.1007/978-3-662-53887-6_31 (Published)

One-round attribute-based key exchange in the multi-party setting, by TIAN, Yangguang; YANG, Guomin; MU, Yi; LIANG, Kaitai; YU, Yong. (2016.0). *Proceedings of the 10th International Conference, Nanjing, China, 2016 November 10–11,* (pp. 227-243) Nanjing, China: Springer Verlag. http://doi.org/10.1007/978-3-319-47422-9_13 (Published)

Achieving IND-CCA security for functional encryption for inner products, by ZHANG, Shiwei; MU, Yi; YANG, Guomin. (2016.0). *Proceedings of the 12th International Conference, Beijing, China, 2016 November 4-6,* (pp. 119-139) Beijing, China: Springer Verlag. http://doi.org/10.1007/978-3-319-54705-3_8 (Published)

Edit distance based encryption and its application, by PHUONG, Tran Viet Xuan; YANG, Guomin; SUSILO, Willy; LIANG, Kaitai. (2016.0). *Proceedings of the 21st Australasian Conference, Melbourne, Australia, 2016 July 4–6,* (pp. 103-119) Melbourne, Australia: Springer Verlag. http://doi.org/10.1007/978-3-319-40367-0_7 (Published)

Linear encryption with keyword search, by ZHANG, Shiwei; YANG, Guomin; MU, Yi. (2016.0). *Proceedings of the 21st Australasian Conference, Melbourne, Australia, 2016 July 4–6,* (pp. 187-203) Melbourne, Australia: Springer Verlag. http://doi.org/10.1007/978-3-319-40367-0_12 (Published)

One-round strong oblivious signature-based envelope, by CHEN, Rongmao; MU, Yi; SUSILO, Willy; YANG, Guomin; GUO, Fuchun; ZHANG, Mingwu. (2016.0). *Proceedings of the 21st Australasian Conference, Melbourne, Australia, 2016 July 4–6,* (pp. 3-20) Melbourne, Australia: Springer Verlag. http://doi.org/10.1007/978-3-319-40367-0_1 (Published)

Recipient revocable identity-based broadcast encryption: How to revoke some recipients in IBBE without knowledge of the plaintext, by SUSILO, Willy; YANG, Guomin; CHEN, Rongmao; MU, Yi; GUO, Fuchun; CHOW, Yang-Wai. (2016.0). *Proceedings of the 11th ACM Asia Conference on Computer and Communications Security, Xi’an, China, 2016 May 30-June 03,* (pp. 201-210) Xi'an: Association for Computing Machinery, Inc. http://doi.org/10.1145/2897845.2897848 (Published)

Strongly leakage-resilient authenticated key exchange, by CHEN, Rongmao; MU, Yi; YANG, Guomin; SUSILO, Willy; GUO, Fuchun. (2016.0). *Proceedings of the The Cryptographers' Track at the RSA Conference 2016, San Francisco, February 29 - March 4,* (pp. 19-36) San Francisco: Springer (part of Springer Nature): Springer Open Choice Hybrid Journals. http://doi.org/10.1007/978-3-319-29485-8_2 (Published)

Attribute based broadcast encryption with short ciphertext and decryption key, by PHUONG, Tran Viet Xuan; YANG, Guomin; SUSILO, Willy; CHEN, Xiaofeng. (2015.0). *Proceedings of the 20th European Symposium on Research in Computer Security, Vienna, Austria, 2015 September 21-25,* (pp. 252-269) Vienna, Austria: Springer Verlag. http://doi.org/10.1007/978-3-319-24177-7_13 (Published)

A new public remote integrity checking scheme with user privacy, by FENG, Yiteng; MU, Yi; YANG, Guomin; LIU, Joseph. (2015.0). *Proceedings of the 20th Australasian Conference, Brisbane, Australia, 2015 June 29 - July 1,* (pp. 377-394) Brisbane, Australia: Springer Verlag. http://doi.org/10.1007/978-3-319-19962-7_22 (Published)

A new general framework for secure public key encryption with keyword search, by CHEN, Rongmao; MU, Yi; YANG, Guomin; GUO, Fuchun; WANG, Xiaofen. (2015.0). *Proceedings of the 20th Australasian Conference, Brisbane, Australia, 2015 June 29 - July 1,* (pp. 59-76) Brisbane, Australia: Springer Verlag. http://doi.org/10.1007/978-3-319-19962-7_4 (Published)

Attribute-based signing right delegation, by LIU, Weiwei; MU, Yi; YANG, Guomin . (2014.0). *Proceedings of the 8th International Conference, Xi'an, China, 2014 October 15–17,* (pp. 323-334) Xi’an, China: Springer Verlag. http://doi.org/10.1007/978-3-319-11698-3_25 (Published)

Efficient hidden vector encryption with constant-size ciphertext, by PHUONG, Tran Viet Xuan; YANG, Guomin; SUSILO, Willy. (2014.0). *Proceedings of the 19th European Symposium on Research in Computer Security, Wroclaw, Poland, 2014 September 7-11,* (pp. 472-487) Wrocław, Poland: Springer Verlag. http://doi.org/10.1007/978-3-319-11203-9_27 (Published)

K-time proxy signature: Formal definition and efficient construction, by LIU, Weiwei; YANG, Guomin; MU, Yi; WEI, Jiannan. (2013.0). *Proceedings of the 7th International Conference, Melaka, Malaysia, 2013 October 23-25,* (pp. 154-164) Melaka, Malaysia: Springer Verlag.

http://doi.org/10.1007/978-3-642-41227-1_9 (Published)

A highly efficient RFID distance bounding protocol without real-time PRF evaluation, by ZHUANG, Yunhui; YANG, Anjia; WONG, Duncan S.; YANG, Guomin; XIE, Qi. (2013.0). *Proceedings of the 7th International Conference, Madrid, Spain, 2013 June 3-4,* (pp. 451-464) Madrid, Spain: Springer Verlag. http://doi.org/10.1007/978-3-642-38631-2_33 (Published)

A new unpredictability-based RFID privacy model, by YANG, Anjia; ZHUANG, Yunhui; WONG, Duncan S.; YANG, Guomin. (2013.0). *Proceedings of the 7th International Conference, Madrid, Spain, 2013 June 3-4,* (pp. 479-492) Madrid, Spain: Springer Verlag. http://doi.org/10.1007/978-3-642-38631-2_35 (Published)

Leakage resilient authenticated key exchange secure in the auxiliary input model, by YANG, Guomin; MU, Yi; SUSILO, Willy; WONG, Duncan S.. (2013.0). *Proceedings of the 9th International Conference, Lanzhou, China, 2013 May 12-14,* (pp. 204-217) Lanzhou, China: Springer Verlag. http://doi.org/10.1007/978-3-642-38033-4_15 (Published)

Cross-domain password-based authenticated key exchange revisited, by CHEN, Liqun; LIM, Hoon Wei; YANG, Guomin. (2013.0). *Proceedings of the 32nd IEEE Conference on Computer Communications, Turin, Italy, 2013 April 14-19,* (pp. 1052-1060) Turin, Italy: IEEE. https://doi.org/10.1109/INFCOM.2013.6566895 (Published)

Strong) multidesignated verifiers signatures secure against rogue key attack, by ZHANG, Yunmei; AU, Man Ho; YANG, Guomin; SUSILO, Willy. (2014.0). *Proceedings of the 6th International Conference, Wuyishan, Fujian, China, 2012 November 21-23,* (pp. 1574-1592) Wuyishan, Fujian, China: Springer. http://doi.org/10.1002/cpe.3094 (Published)

Strongly secure certificateless key exchange without pairing, by YANG, Guomin; TAN, Chik How . (2011.0). *Proceedings of the 6th ACM Symposium on Information, Compuer and Communications Security, Hong Kong, China, 2011 March 22-24,* (pp. 71-79) Hong Kong, China: ACM. http://doi.org/10.1145/1966913 (Published)

Authenticated key exchange under bad randomness, by YANG, Guomin; DUAN, Shanshan; WONG, Duncan S.; TAN, Chik How; WANG, Huaxiong
. (2011.0). *Financial Cryptography and Data Security: 15th International Conference, FC 2011, Gros Islet, St. Lucia, February 28 - March 4: Proceedings,* (pp. 113-126) Cham: Springer. https://doi.org/10.1007/978-3-642-27576-0_10 (Published)

Dynamic group key exchange revisited, by YANG, Guomin; TAN, Chik How. (2010.0). *Cryptology and Network Security: 9th International Conference, CANS 2010, Kuala Lumpur, Malaysia, December 12-14: Proceedings,* (pp. 261-277) Cham: Springer. https://doi.org/10.1007/978-3-642-17619-7_19 (Published)

Probabilistic public key encryption with equality test, by YANG, Guomin; TAN, Chik How; HUANG, Qiong; WONG, Duncan S.. (2010.0). *Topics in Cryptology: Cryptographers' Track at the RSA Conference, CT-RSA 2010, San Francisco, March 1-5: Proceedings,* (pp. 119-131) Cham: Springer. https://doi.org/10.1007/978-3-642-11925-5_9 (Published)

Efficient non-interactive range proof, by YUEN, Tsz Hon; HUANG, Qiong; MU, Yi; SUSILO, Willy; WONG, Duncan S.; YANG, Guomin. (2009.0). *Proceedings of the 15thAnnual International Conference, Niagara Falls, USA, 2009 July 13-15,* (pp. 138-147) Niagara Falls: Springer Verlag. http://doi.org/10.1007/978-3-642-02882-3_15 (Published)

Ambiguous optimistic fair exchange, by HUANG, Qiong; YANG, Guomin; WONG, Duncan S.; SUSILO, Willy. (2008.0). *Proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security, Melbourne, Australia, 2008 December 7-11*, (pp. 74-89) Melbourne, Australia: Springer Verlag. http://doi.org/10.1007/978-3-540-89255-7_6 (Published)

Traceable and retrievable identity-based encryption, by AU, Man Ho; HUANG, Qiong; LIU, Joseph K.; SUSILO, Willy; WONG, Duncan S.; YANG, Guomin . (2008.0). *Applied Cryptography and Network Security: 6th International Conference, ACNS 2008, New York, June 3-6: Proceedings,* (pp. 94-110) Cham: Springer. https://doi.org/10.1007/978-3-540-68914-0_6 (Published)

Efficient optimistic fair exchange secure in the multi-user setting and chosen-key model without random oracles, by HUANG, Qiong; YANG, Guomin; WONG, Duncan S.; SUSILO, Willy. (2008.0). *Proceedings of the Cryptographers' Track at the RSA Conference 2008, San Francisco, April 8-11,* (pp. 106-120) San Francisco: Springer Verlag. http://doi.org/10.1007/978-3-540-79263-5_7 (Published)

Time capsule signature: Efficient and provably secure constructions, by HU, Bessie C.; WONG, Duncan S.; HUANG, Qiong; YANG, Guomin; DENG, Xiaotie . (2007.0). *Public Key Infrastructure: 4th European PKI Workshop: Theory and Practice, Palma de Mallorca, Spain, June 28-30: Proceedings,* (pp. 127-142) Cham: Springer. https://doi.org/10.1007/978-3-540-73408-6_9 (Published)

A more natural way to construct identity-based identification schemes, by YANG, Guomin; CHEN, Jing; WONG, Duncan S.; DENG, Xiaotie; WANG, Dongsheng. (2007.0). *Applied Cryptography and Network Security: 5th International Conference, ACNS 2007, Zhuhai, China, June 5-8: Proceedings ,* (pp. 307-322) Cham: Springer. https://doi.org/10.1007/978-3-540-72738-5_20 (Published)

Malicious KGC attacks in certificateless cryptography, by AU, Man Ho; CHEN, Jing; LIU, Joseph K.; MU, Yi; WONG, Duncan S.; YANG, Guomin. (2007.0). *Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security, Singapore, 2007 March 20-22,* (pp. 302-311) Singapore: ACM. http://doi.org/10.1145/1229285.1266997 (Published)

Formal analysis and systematic construction of two-factor authentication scheme, by YANG, Guomin; WONG, Duncan S.; WANG, Huaxiong; DENG, Xiaotie. (2006.0). *Information and Communications Security: 8th International Conference, ICIS 2006, Raleigh, NC, December 4-7: Proceedings,* (pp. 82-91) Cham: Springer. https://doi.org/10.1007/11935308_7 (Published)

Anonymous signature schemes, by YANG, Guomin; WONG, Duncan S.; DENG, Xiaotie; WANG, Huaxiong . (2006.0). *Public Key Cryptography: 9th International Conference on Theory and Practice of Public-Key Cryptography, PKC 2006, New York, April 24-26,* (pp. 347-363) Cham: Springer. https://doi.org/10.1007/11745853_23 (Published)

Deposit-case attack against secure roaming, by YANG, Guomin; WONG, Duncan S.; DENG, Xiaotie . (2005.0). *Information Security and Privacy: 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4-6: Proceedings,* (pp. 417-428) Cham: Springer. https://doi.org/10.1007/11506157_35 (Published)

Efficient anonymous roaming and its security analysis, by YANG, Guomin; WONG, Duncan S.; DENG, Xiaotie. (2005.0). *Applied Cryptography and Network Security: 3rd International Conference, ACNS 2005, New York, June 7-10: Proceedings,* (pp. 334-349) Cham: Springer. https://doi.org/10.1007/11496137_23 (Published)

Research Grants

Singapore Management University

Trusted Decentralized Identities, Digital Trust Centre (DTC) Research Grant, National Research Foundation (NRF) , PI (Project Level): YANG Guomin , Co-PI (Project Level): Robert H DENG

Privacy Preserving Self-Sovereign Digital Identity, SMU Internal Grant, Ministry of Education (MOE) Tier 1 , PI (Project Level): YANG Guomin, 2022, S$97,562.15

Other Institutions

Securing Public Cloud Storage with Protection against Malicious Senders, ARC Discovery Project, Australia Research Council Co-PI (Project Level): YANG Guomin

Efficient Multi-key Homomorphic Encryption and Its Applications, ARC Linkage Project, Australia Research Council Co-PI (Project Level): YANG Guomin

On the Structure of Lattices for Post-Quantum Cryptography, Measurement Science and Engineering Research Grant Programme, National Institute of Standards and Technology Co-PI (Project Level): YANG Guomin

Real Time Visualisation of Intrusion Detection and Behavioural Analytics Data for Combatting Cyber Attacks, Pilot Grant Scheme, NSW Cyber Security Network Co-PI (Project Level): YANG Guomin

Leakage-resilient and Quantum-secure Authenticated Key Exchange Protocol, ARC DECRA Project, Australia Research Council PI (Project Level): YANG Guomin

Post-Quantum Cryptology: New Approach and Investigation, General Research Fund, Australia National

Security Science and Technology Centre Co-PI (Project Level): YANG Guomin

TEACHING

Courses Taught

Singapore Management University

Undergraduate Programmes :

- Data Security and Privacy
- Foundations of Cybersecurity
- Introduction to Programming

Postgraduate Research Programmes :

- Empirical Research Project 1

THESES AND DISSERTATIONS

Theses and Dissertations Supervised

Other Institutions

Supervisor, "Searchable Encryption for Cloud and Distributed Systems", Thesis by LIU Xueqiao, University of Wollongong, 2017

Supervisor, "Privacy-preserving Cryptographic Solutions for Cloud Storage", Thesis by WU Tong, University of Wollongong, 2016

Supervisor, "Practical revocable cryptographic schemes for cloud-based applications", Thesis by XU Shengmin, University of Wollongong, 2015

Supervisor, "Privacy-enhanced key management for distributed systems", Thesis by TIAN Yangguang, University of Wollongong, 2013

Supervisor, "Contributions to Privacy-Preserving Digital Signatures and Their Applications", Thesis by WEI Jiannan, University of Wollongong, 2012

Theses and Dissertations Assessed

Other Institutions

Co Supervisor, "Contributions to Blockchain-Based Security Protocols", Thesis by LI Yannan, University of Wollongong, 2017

Co Supervisor, "New Conditional Privacy-preserving Encryption Schemes in Communication Network", Thesis by YAO Zhongyuan, University of Wollongong, 2014

Co Supervisor, "Practical functional encryption techniques and their applications", Thesis by ZHANG Shiwei, University of Wollongong, 2014

Co Supervisor, "Secure Data Storage and Retrieval in Cloud Computing", Thesis by CHEN Rongmao, University of Wollongong, 2013

Co Supervisor, "Attribute-Based Encryption Schemes", Thesis by PHUONG Tran Viet Xuan, University of Wollongong, 2013

Co Supervisor, "Contributions to Cryptography with Restricted Conditions", Thesis by LIU Weiwei, University of Wollongong, 2012

EXTERNAL SERVICE – PROFESSIONAL

Committee Member, 6th IEEE Conference on Dependable and Secure Computing, 2023

Committee Member, 18th ACM ASIA Conference on Computer and Communications Security, 2023

Committee Member, 28th Australasian Conference on Information Security and Privacy, 2023

Conference Chair, 27th Australasian Conference on Information Security and Privacy, 2022

Committee Member, 27th European Symposium on Research in Computer Security, 2022

Committee Member, JTC 1/SC 27/WG 2, ISO/IEC, 2018 - 2022

Editor Associate Editor, Theoretical Computer Science Journal, 2018 - Present